Intro to Discrete Structures Lecture 6

Pawel M. Wocjan

School of Electrical Engineering and Computer Science

University of Central Florida

wocjan@eecs.ucf.edu

Hints for HW1

$$((p \to q) \wedge (q \to r)) \to (p \to r)$$

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore\ p \to r \end{array}$$

use $\boxed{p \to q \equiv \neg p \vee q}$

proposition1 LAW

LAW $\equiv$ proposition2

$\equiv$

$\equiv$

$\equiv$

$\vdots$

Hints for HW1

No student is a monkey.

Domain the set of all ~~students~~ people

$M(x)$: ~~student~~ x is a monkey

$\neg \exists x \; M(x) \equiv \forall x \neg M(x)$

$S(x)$ person x is a student

$\neg \exists x \; S(x) \wedge \neg M(x) \equiv \forall x \neg (S(x) \wedge \neg M(x))$

$\equiv \forall x \neg S(x) \vee M(x) \equiv \forall x \, S(x) \rightarrow \neg M(x)$

Formal Notation & Meaning

- Let $p_1, p_2, \ldots, p_n$ and c be (compound) propositions. The notation

$$\begin{array}{rl} & p_1 \\ & p_2 \\ & \vdots \\ & p_n \\ \hline \therefore & c \end{array}$$

means

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow c \equiv \mathsf{T}.$$

- $p_1, p_2, \ldots, p_n$ are called the premises and c is called the conclusion.

I. Rules of Inference

- Modus ponens

$$\begin{array}{rl} & p \\ & p \to q \\ \hline \therefore & q \end{array}$$

- Modus tollens

$$\begin{array}{rl} & \neg q \\ & p \to q \\ \hline \therefore & \neg p \end{array}$$

Modus Ponens – Modus Tollens

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$$

$$\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore \neg p \end{array} \equiv \neg q \to \neg p$$

II. Rules of Inference

- Hypothetical syllogism

$$\begin{array}{rr} & p \rightarrow q \\ & q \rightarrow r \\ \hline \therefore & p \rightarrow r \end{array}$$

- Disjuctive syllogism

$$\begin{array}{rr} & p \vee q \\ & \neg p \\ \hline \therefore & q \end{array}$$

Modus Ponens – Disjunctive syllogism

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$$

$$p \vee q \equiv \neg p \to q$$

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

III. Rules of Inference

- Addition

$$\begin{array}{ll} & p \\ \hline \therefore & p \vee q \end{array}$$

- Simplification

$$\begin{array}{ll} & p \wedge q \\ \hline \therefore & p \end{array}$$

IV. Rules of Inference

- Conjunction

$$\begin{array}{rl} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$$

$(p \wedge q) \to (p \wedge q) \equiv T$

- Resolution

$$\begin{array}{rl} & p \vee q \\ & \neg p \vee r \\ \hline \therefore & q \vee r \end{array}$$

Resolution

- The inference rule "resolution"

$$\begin{array}{rl} & p \vee q \\ & \neg p \vee r \\ \hline \therefore & q \vee r \end{array}$$

  is based on the tautology

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)\,.$$

- We recover disjunctive syllogism by setting $r = F$

$$((p \vee q) \wedge (\neg p)) \rightarrow q\,.$$

Hypothetical Syllogism – Resolution

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore\ p \rightarrow r \end{array}$$

$$\begin{array}{ll} p \vee q & \equiv \neg q \rightarrow p \\ \neg p \vee r & \equiv p \rightarrow r \\ \hline q \vee r & \equiv \neg q \rightarrow r \end{array}$$

Hypothetical Syllogism – Resolution

Rules of Inference for Quantified Statements

- Universal instantiation

$$\begin{array}{rl} & \forall x P(x) \\ \hline \therefore & P(c) \end{array}$$

- Universal generalization

$$\begin{array}{rl} & P(c) \text{ for an arbitrary } c \\ \hline \therefore & \forall x P(x) \end{array}$$

Rules of Inference for Quantified Statements

- Existential instantiation

$$\frac{\exists x P(x)}{\therefore \quad P(c) \text{ for some element } c}$$

- Existential generalization

$$\frac{P(c) \text{ for an some element } c}{\therefore \quad \exists x P(x)}$$

Universal Modus Ponens

- Universal Modus Ponens

$$\begin{array}{ll} & \forall x(P(x) \rightarrow Q(x)) \\ & P(a)\text{, where } a \text{ is a particular element in the domain} \\ \hline \therefore & Q(a) \end{array}$$

All Greeks are Mortal $\forall x(G(x) \rightarrow M(x))$

Sokrates is a Greek $G(\text{Sokrates})$

Therefore, Sokrates is mortal. $\therefore M(\text{Sokrates})$

UMP in Math

- Assume that the statement

  "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n"

  is true. Use UMP to show that $100^2 < 2^{100}$.

$P(n)$: $n > 4$

$Q(n)$: $n^2 < 2^n$

$\forall n \, (P(n) \to Q(n))$

$P(100)$

$\therefore Q(100)$

$P(100)$ is T

Universal Modus Tollens

- Universal Modus Tollens

$$\begin{array}{rl} & \forall x(P(x) \to Q(x)) \\ & \neg Q(a)\,,\ \text{where } a \text{ is a particular element in the domain} \\ \hline \therefore & \neg P(a) \end{array}$$

Introduction to Proofs

- Some Terminology
  - Axiom (or Postulate)
  - Theorem
  - Proposition
  - Lemma (Lemmas or Lemmata)
  - Corollary
  - Proof
  - Conjecture

Proofs Methods

- Direct Proof
- Proof by Contraposition (or Indirect Proof)
- Proof by Contradition
- Proof by Induction

Direct Proof

Definition 1: The integer n is **even** if there exists an integer k such that $n = 2k$, and n is **odd** if there exists an integer k such that $n = 2k + 1$.

Example 1: Give a direct proof of the theorem "If n is odd, then n^2 is odd."

Proof: assume n is odd $\Rightarrow \exists k \;\; n = 2k+1$

$\Rightarrow \exists k \;\; n^2 = (2k+1)^2 = (2k)^2 + 2(2k) + 1^2$

$= 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

$= 2\ell + 1$ where $\ell = 2k^2 + 2k$

Def

$\Rightarrow n^2$ is odd

Direct Proof

Definition: An integer a is a perfect square if there is an integer b such that $a = b^2$.

Example 2: Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

$m = r^2$
$n = s^2$ r, s are integers

$\Rightarrow m \cdot n = r^2 \cdot s^2 = (rs)^2 = t^2$ where

$t = rs$

Indirect Proof

Example 3: Prove that if n is an integer and $3n+2$ is odd, then n is odd.

The direct approach does not work!

$3n+2$ is odd $\Rightarrow 3n+2 = 2k+1$

for some integer k

Indirect Proof

Example 3: Prove that if n is an integer and $3n+2$ is odd, then n is odd.

Use contraposition!

$$\forall n \in \mathbb{N}\, \big(\mathrm{odd}(3n+2) \rightarrow \mathrm{odd}(n)\big)$$

$$\equiv \forall n \in \mathbb{N}\, \big(\neg \mathrm{odd}(n) \rightarrow \neg \mathrm{odd}(3n+2)\big)$$

$$\equiv \forall n \in \mathbb{N}\, \big(\mathrm{even}(n) \rightarrow \mathrm{even}(3n+2)\big)$$

n even $\Rightarrow n = 2k$ for some integer k

$\Rightarrow 3n+2 = 3(2k)+2 = 6k+2$

$= 2(3k+1)$

$\Rightarrow 3n+2$ is even $\quad = 2\ell$ where $\ell = 3k+1$

Indirect Proof

Example 4: Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ ~~and~~ or $b \leq \sqrt{n}$.

$n = ab \Rightarrow a \leq \sqrt{n} \lor b \leq \sqrt{n}$

assume that $a \leq \sqrt{n}$ ~~and~~ $\lor$ $b \leq \sqrt{n}$ is false

$\neg(a \leq \sqrt{n} \lor b \leq \sqrt{n})$ is true

$\Rightarrow a > \sqrt{n} \land b > \sqrt{n}$

$\Rightarrow ab > \sqrt{n}\sqrt{n} > n$

$\Rightarrow ab \neq n$

$p \rightarrow q$

$\neg q \rightarrow \neg p$

Proof Strategy

- We have seen two important methods for proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$.

  These two methods are

  - the direct proof and
  - the indirect proof

  methods.

- It takes some practice (solving homework problems) to learn to recognize quickly the correct approach.

- Try first the direct approach. If it does not work then try the indirect approach.

END OF LEC 6

Direct or Indirect Proof?

Definition: The real number r is **rational** if there exist integers p and q with $q \neq 0$ such that $r = p/q$.

Example 7: Prove that the sum of two rational numbers is rational.

Direct or Indirect Proof?

Example 8: Prove that if n is an integer and n^2 is odd, then n is odd.

Proof by Contradition

- We can prove that p is true if we can show that $\neg p \rightarrow (r \vee \neg r)$ is true for some proposition r.